

REMARKS

In response to the Official Action of June 1, 2005, claim 65 has been amended in a manner as suggested by the Examiner at paragraph 4 of the Official Action. Also, claim 30 has been amended to correct an error regarding the last element wherein the device is of the second system rather than the first system. Claim 56 has been amended to correct a grammatical error. Finally, claim 58 has been amended to correct an antecedent basis problem with the recited key. For the reasons set forth below, it is respectfully submitted that claims 1-65 of the present application, as amended, are allowable.

Preliminarily referring now to paragraph 2 of the Official Action, the Examiner states that an oath or declaration identifying this application by application number and filing date is missing. Please note that a declaration was filed on May 6, 2002 in response to a Notice to File Missing Parts of Nonprovisional Application; a copy of the response is enclosed for the Examiner's reference as Attachment A. Also forming part of Attachment A is a copy of the return postcard submitted with the response which shows that the declaration and filing fee were received at the U.S. Patent and Trademark Office on May 20, 2002.

Referring now to paragraphs 3 and 4 of the Official Action, claim 65 has been amended in a manner as suggested by the Examiner and therefore it is believed to be in compliance with 35 U.S.C. §101.

Referring now to paragraphs 5 and 6 of the Official Action, it is respectfully submitted that claims 1-9, 11, 12, 14, 17-23, 26, 27, 29-38, 40, 41, 43, 46-52, 55, 56, 58-63 and 65, as amended are believed to be neither anticipated nor

suggested by US patent 6,209,091, Sudia et al (hereinafter Sudia). The Examiner specifically points to column 6, lines 54-65, column 14, lines 4-7, column 13, line 66 through column 14, line 4 and column 14, lines 14-26 for supporting the conclusion that claims 1, 29 and 58 are taught by Sudia. Applicant's attorney respectfully submits that the recited portions of Sudia do not anticipate or suggest claims 1, 29 or 58.

Specifically with regard to claim 1, it is directed to a method of authenticating a user of a second system where that user has an authenticated identity in a first system. The steps of the method comprise the second system causing a key to be generated for use in the second system, the second system generating a certificate for the key and the signing of the certificate for the key using the authenticated identity of the user in the first system. It is clear from a reading of Sudia that it is directed to a multi-step signing system and method which uses multiple signing devices to affix a single signature which can be verified using a single public verification key. Figure 1 of Sudia is an overview of the basic architecture for an operational signing system and as explained at column 6, line 54 through column 7, line 3, comprises a plurality of authorizing agents 1a, 2a, 3a, 4a and 5a with a corresponding plurality of signing devices 1, 2, 3, 4 and 5. As set forth at column 2, lines 52-65 of Sudia, the multi-step signing system uses a public key cryptosystem approach to sign an electronic document such that a recipient of the document can verify the signature using a public verification key of the signer. However, the private signature key which corresponds to the public verification key is not permitted to exist in whole, available form in one place at any time during the normal signing operation. Rather, as explained in the summary, a private

signature key consists of what are termed “operational shares” which can be used to affix or modify a partial signature and sequential operation of multiple shares produces a signature that can be verified using the public verification key. The full signature is not completed until all, or some portion of all, of the signing devices have signed. Furthermore, each signing device requires authorization from all or some number of its associated authorizing agents before participating in the signature process.

With regard to what the Examiner states is the second system causing a key to be generated for use in the second system, reference is made to column 14, lines 4-7. However, a reading of the steps starting at column 13, line 66 through column 14, line 34 makes clear that Signing Device (2) affixes a partial system-wide authority (SWA) signature using its own SWA signature key share (93) (see column 14, lines 14-15). Furthermore, signing device (2) then sends the partially signed certificate (105) to signing device (3) (see column 14, lines 35-36). Then signing device (3) completes the system-wide authority signature by exponentiating the already-applied partial signature --SD2 as set forth at column 14, lines 35-49. Then, signing device (3) returns the signed certificate (107) to signing device (1) which then distributes copies of the certificate to the other signing devices thereby allowing them to verify its future signatures. All of these steps in Sudia are with reference to recertification of the signing device. The signing of certificate (107) of Signing Device (1) uses the same multi-step process used to affix a single signature by use of partial signing by multiple signing devices which can be verified by a single public verification key (see columns 14, lines 63-67).

It is further stated at column 14, lines 54-57 that any combination of signing devices may sign in any order so as to produce the same signature. Thus, the very purpose to which Sudia is directed is completely different from the claimed invention as set forth in method claim 1. There is no teaching or suggestion in Sudia of a user of a second system authenticating its identity by having an authenticated identity in a first system. What Sudia is directed to is a technique in which a partial SWA signature uses the SWA signature key share of multiple signing devices in order to generate a signed certificate. This is made clear in the abstract of Sudia wherein it states:

“Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents. In a serial embodiment, after a first partial signature has been affixed, a second signing device exponentiates the first partial signature. In a parallel embodiment each signing device affixes a partial signature, and the plurality of partial signatures are multiplied together to form the final signature. Security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices and by distributing authority to affix a partial signature among a plurality of authorizing agents.”

Clearly, there is no counterpart in the present invention to a plurality of signing devices and a distributing authority to affix a partial signature among a plurality of authorizing agents. In the present invention as claimed in claim 1, the signing of the certificate for the key in the second system uses the authenticated identity of the user in the first system. In Sudia, there is no signing of a certificate

for a key in a second system using the authenticated identity of the user in a first system. The reason for this is quite simple; Sudia is directed to enhancing security through use of a multi-step digital signature system so that no one signing device is able to affix a single signature which can be verified using a single public verification key. Therefore, each of Sudia's signing devices possesses a share of a signature key and affixes a partial signature in response to authorization wherein that authorization is obtained from a plurality of authorizing agents.

Again, the method of authenticating a user of a second system where the user has an authenticated identity in a first system as set forth in claim 1 of the present invention, does not use a plurality of authorizing agents to allow the second system to sign the certificate for the key of that second system. Rather, the present invention is directed to the straightforward concept of allowing a user of a second system to use its authenticated identity in a first system to authenticate a certificate for a key in the second system. Sudia is silent with regard to such a method and therefore it is respectfully submitted that it does not disclose or suggest claim 1 of the present application.

Method claim 29, which is directed to a method of authenticating a user in a network environment where the user has an authenticated identity not associated with said network environment, is believed to be distinguished over Sudia for the same reasons as set forth above with regard to method claim 1. Furthermore, the system recited in independent claim 58 is similar to method claim 29 and method claim 1 in that it claims a system for authenticating a user in a network environment where the user has an authenticated identity not associated with that network environment and further has means for generating a certificate for a key in

said network environment and means for signing the certificate for the key using the user's authenticated identity which is not associated with said network environment. Therefore, claim 58 is believed to be neither anticipated nor suggested by Sudia. Please note that claim 58 has been amended to make clear that the key in the first recited element is in fact a key in the recited network environment.

Since claim 1 is believed to be distinguished over Sudia, it is respectfully submitted that claims 2-28, which all ultimately depend from claim 1 are also distinguished over Sudia due to their dependency from claim 1.

Independent system claim 30 is also rejected as anticipated in view of Sudia for the reasons set forth at page 3, line 16 through page 4, line 10. Claim 30 is directed to a system which is similar to method claim 1, but which further recites additional details concerning the second device which forms part of the first system; namely, that the second device has means for storing information regarding the authenticated identify of the user in the first system, as well as means for communicating said information and wherein the device of the first system has means for receipt of said information from the second device and further has means for signing the certificate generated in the second system using the authenticated identify of the user in the first system. Again, for reasons similar to those presented with regard to claims 1, 29 and 58, it is respectfully submitted that claim 30 is neither disclosed nor suggested by Sudia.

Thus, even though Signing Device (1) generates an unsigned certificate (103) and transmits that certificate to Signing Device (2) in Sudia (see column 13, lines 66-67) and even though the unsigned certificate includes the signing device's

identity and a public signature verification key for the device's signature key, this unsigned certificate is not used by a device forming part of a second system (which the Examiner equates to the Signing Device (2) in Sudia) for signing a certificate for the key generated by the device of the second system using the authenticated identity of the user in the first system. At best, the second Signing Device (2) in Sudia simply affixes a partial SWA signature using its own SWA signature key share (93) (not the first Signing Device key) which in turn is then sent to the next signing device (Signing Device (3)) for completing a system-wide authority signature by exponentiating the already-applied partial signature --SD2 (see column 14, lines 14-39).

It is therefore respectfully submitted that claim 30 is neither disclosed nor suggested by Sudia. Since claim 30 is believed to be distinguished over Sudia, it is respectfully submitted that claims 31-57, all of which ultimately depend from claim 30, are further distinguished over Sudia.

Independent device claim 59 is also rejected as anticipated by Sudia for the reasons set forth at page 4, line 11 through page 5, line 1 of the Official Action. The device recited in claim 59 is similar to system claim 30 with some minor variations. Thus, the device recited in claim 59 has means for generating a key for use in a second system, as well as means for generating a certificate for that key and means for transferring the certificate to a device forming part of the first system wherein the user of the first system as an authenticated identify and further wherein the device of the first system has information concerning the authenticated identity of the user in the first system so as to sign the certificate generated by the second system using the authenticated identity of the user in the

first system. Claim 59 further recites that the device of the second system further comprises means for receipt of the signed certificate and means for transferring the signed certificate to a third party of the second system.

The additional means of the device to the second system so as to receive the signed certificate and to transfer the signed certificate to a third party adds additional limitations to the concepts previously discussed and, for similar reasons, it is believed to be further distinguished over Sudia.

Thus, even though Sudia discloses Signing Device (2) sending a partially signed certificate to Signing Device (3) and Signing Device (3) completing a system-wide authority signature by exponentiating the already-applied partial signature, such sending of partially signed certificates does not disclose or suggest claim 59, wherein a device of the second system comprises means for receipt of the signed certificate, wherein the signed certificate is based upon the authenticated identity of the user in the first system and further wherein the device of the second system transfers that signed certificate to a third party of the second system.

The Examiner takes the position that the device of the second system is equated to device (1) shown in Figure 1 of Sudia and that device (1) has means for transferring the signed certificate to a third party of the second system, citing column 15, lines 16-19. However, column 15, lines 16-19 simply says that the signing devices will affix the system-wide authority official signature to authorizing agent certificates, thus certifying a public signature verification key for each authorizing agent. It is not seen how the affixing of a system-wide authority official

signature to authorizing agent certificates equates to means for transferring the signed certificate to a third party of said second system as recited in claim 59.

In short, the underlying concept embodied in claim 59 is the fact that the user has an authenticated identity in a first system and further that a certificate which is generated by a second system is signed by the authenticated identity of the user in the first system. Sudia's multi-step signing system and method which uses multiple signing devices to affix a single signature so that each signing device only possesses a share of the signature key and affixes a partial signature in response to an authorization from a plurality of authorizing agents, is neither anticipatory nor suggestive of the device recited in claim 59.

Claim 60 is also rejected as anticipated in view of Sudia. Claim 60 is directed to a wireless device for use in authenticating a user of a second system where the user has an authenticated identity in a first system associated with the wireless device and further wherein the second system includes a device having means for causing a key to be generated for use in the second system, means for generating a certificate for that key and means for transferring the certificate to another device. Again, the wireless device recited in claim 60 has means for signing the certificate generated in the second system using the authenticated identity of the user in the first system. For the reasons set forth above with regard to the previously discussed independent claims, it is respectfully submitted that claim 60 is neither disclosed nor suggested by Sudia.

Furthermore, Sudia is not directed specifically to a wireless device, contrary to the position asserted by the Examiner by reference to column 9, lines 51-57 of Sudia. The recited portion of Sudia simply states that signing devices encrypt their

communications using a public/private cryptographic scheme. No mention of wireless devices is set forth in the recited portion of Sudia. It is therefore respectfully submitted that independent claim 60 is further distinguished over Sudia.

Since claim 60 is believed to be distinguished over Sudia, it is also respectfully submitted that claims 61-64, which all ultimately depend from claim 60, are further distinguished over Sudia.

Finally, independent claim 65 is directed to a program stored on a computer readable medium for execution by a processor for implementing the authentication of a user of a second system where the user has an authenticated identify in a first system. The recited elements are similar to method claim 1 and claims 59 and 60. For similar reasons, it is respectfully submitted that claim 65 is distinguished over Sudia.

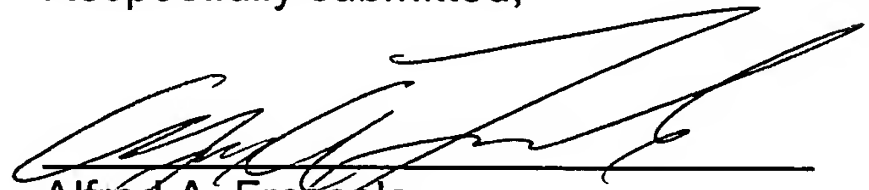
The remaining dependent claims rejected in paragraph 6 of the Official Action have been discussed and are believed to be distinguished over Sudia. Furthermore, the remaining dependent claims rejected under 35 U.S.C. §103 at paragraphs 7-9 of the Official Action, in view of Sudia and additional prior art, are believed to be distinguished over the cited art due to their dependency from independent claims which are believed to be distinguished over the art.

It is therefore respectfully submitted that claims 1-65, as amended, are believed to be distinguished over the cited art and that the claims are therefore in condition for allowance. Such action is earnestly solicited.

Respectfully submitted,

Dated: September 1, 2005

WARE, FRESSOLA, VAN DER
SLUYS & ADOLPHSON LLP
Building Five, Bradford Green
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955



Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550

19217

WARE, FRESSOLA
VAN DER SLUYS & ADOLPHSON LLP
755 MAIN STREET, BLDG. 5
MONROE, CT 06468
(203) 261-1234

PEOPLE'S BANK
51-7218-2211

PAY TWO THOUSAND FIFTY-SIX AND NO/100
TO THE
ORDER OF

DATE

AMOUNT

05/06/02

\$2,056.00

Commissioner of Patents & Trademarks
944-005-002

Will J. Parker

⑈019217⑈ ⑆221172186⑆ 032 7006860⑈

WARE, FRESSOLA
VAN DER SLUYS & ADOLPHSON LLP

19217

19217
05/06/02

Commissioner of Patents & Trademarks

\$2,056.00

INVOICE # 050602

944-005-002





Applicant Paatero
For: Method and System for User Generated Keys and Certificates
Serial No. 10/090,422 Filed: February 28, 2002

The following papers were received in the U.S. Patent and Trademark Office:

<input checked="" type="checkbox"/> Transmittal of Completion of Filing	<input type="checkbox"/> Amendment and/or Response
<input type="checkbox"/> Specification - No. of Pages <u>Req.</u>	<input type="checkbox"/> Info. Disclosure Statement
<input type="checkbox"/> Claims - No. of Pages	<input type="checkbox"/> TM or SM Appl. - No. of Pages
<input type="checkbox"/> Abstract - No. of Pages	<input type="checkbox"/> Specimens - No. of
<input checked="" type="checkbox"/> Decl. and Power of Atty.	<input checked="" type="checkbox"/> Fee: \$1972.00 Enclosed
<input checked="" type="checkbox"/> Assignment w/cover sheet	<input type="checkbox"/> Drawings - No. of Sheets
<input type="checkbox"/> Small Entity Statement	
<input checked="" type="checkbox"/> Copy of Notice	
<input checked="" type="checkbox"/> PTO Letter regarding error in	
<input type="checkbox"/> Small Entity Status	

Attorney: AAF/aks Date Mailed: 5/6/02
Please date stamp and return

Docket No.
944-005.2



RECEIVED
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON

MAY 28 2002

FILE 944-005.2
ANS'D. any

Applicant Paatero
Inventor Method and System for User Generated Keys and Certificates
Serial No. 10/090,422 Filed: February 28, 2002



The following papers were received in the U.S. Patent and Trademark Office:

☒ Transmittal of Completion of Filing _____ Amendment and/or Response
_____ Specification - No. of Pages _____ Req. _____ Info. Disclosure Statement
_____ Claims - No. of Pages _____ TM or SM Appl. - No. of Pages _____
_____ Abstract - No. of Pages _____ Specimens - No. of _____
☒ Decl. and Power of Atty. _____ ☒ Fee: \$1972.00 Enclosed
☒ Assignment w/cover sheet _____ Drawings - No. of Sheets _____
_____ Small Entity Statement _____
☒ Copy of Notice _____
☒ PTO Letter regarding error in _____
_____ Small Entity Status _____

OFFICE

No. 6221

certificates

Attorney: _____ Date Mailed: _____ Docket No. _____
JAF/aks 5/6/02 944-005.2
Please date stamp and return

(check and complete this item, if applicable)

- I. ☒ This replies to the Notice to File Missing Parts of Application (PTO-1533) mailed April 4, 2002

NOTE: If these papers are filed before the office letter issues, adequate identification of the original papers should be made, e.g., in addition to the name of the inventor and title of invention, the filing date based on the "Express Mail" procedure, the serial number from the return post card or the attorney's docket number added.

- ☒ A copy of the Notice to File Missing Parts of Application—Filing Date Granted (Form PTO-1533) is enclosed.

NOTE: The PTO requires that a copy of Form PTO-1533 be returned with the response to the notice to file missing parts to the application.

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

- ☒ deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

FACSIMILE

- ☐ transmitted by facsimile to the Patent and Trademark Office.

Date: 5/6/02

Anita Schelmetic

Signature

Anita Schelmetic

(type or print name of person certifying)

(Completion of Filing Requirements — Nonprovisional Application [5-1]—page 1 of 6)



PATENT
944-005.2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the matter of:	Paatero)	
)	
Serial No:	10/090,422)	Group Art Unit: 2681
)	Examiner:
Filed:	February 28, 2002)	Confirm. No. 6221
)	
For:	Method and System for User)	
	Generated Keys and Certificates)	

COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

Please note that the Notice to File Missing Parts of Nonprovisional Application dated April 4, 2002 is in error in that it indicates the application to be a small entity. This application was filed as a large entity and the fees paid in response to the Notice to File Missing Parts of Nonprovisional Application are being paid as a large entity.

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patents, Washington, D.C. 20231

Anita Scheltnie

Date: May 6, 2002

There is also an error in the count of the independent claims. The Notice to File Missing Parts of Nonprovisional Application states there are three independent claims over three, wherein there are actually four independent claims over three. The fee being submitted is for a large entity and for the correct number of extra claims.

Respectfully submitted,

Date: 5/6/02



Alfred A. Fressola, Reg. No. 27,550
Ware, Fressola, Van Der Sluys
& Adolphson LLP
Bradford Green, Building Five
755 Main Street, PO Box 224
Monroe, CT 06468
(203) 261-1234



Practitioner's Docket No. 944-005.2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Paatero

Application No.: 10 /090,422 Group No.: 2681 Conf. No. 6221

Filed: February 28, 2002 Examiner:

For: Method and System for User Generated Keys and Certificates

Box Missing Part
Assistant Commissioner for Patents
Washington, D.C. 20231

**COMPLETION OF FILING REQUIREMENTS
— NONPROVISIONAL APPLICATION**

(check and complete this item, if applicable)

- I. ☒ This replies to the Notice to File Missing Parts of Application (PTO-1533) mailed April 4, 2002

NOTE: If these papers are filed before the office letter issues, adequate identification of the original papers should be made, e.g., in addition to the name of the inventor and title of invention, the filing date based on the "Express Mail" procedure, the serial number from the return post card or the attorney's docket number added.

- ☒ A copy of the Notice to File Missing Parts of Application—Filing Date Granted (Form PTO-1533) is enclosed.

NOTE: The PTO requires that a copy of Form PTO-1533 be returned with the response to the notice to file missing parts to the application.

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

- ☒ deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

FACSIMILE

- ☐ transmitted by facsimile to the Patent and Trademark Office.

Date: 5/6/02

Anita Schelmetic

Signature

Anita Schelmetic

(type or print name of person certifying)

DECLARATION OR OATH

- II. ☒ No declaration or oath was filed. Enclosed is the original declaration or oath for this application.

NOTE: If the correct inventor or inventors are not named on filing a nonprovisional application under § 1.53(b) without an executed oath or declaration under § 1.63, the later submission of an executed oath or declaration under § 1.63 during the pendency of the application will act to correct the earlier identification of inventorship. 37 C.F.R. § 1.48(f)(1).

OR

- ☐ The declaration or oath that was filed was determined to be defective. A new original oath or declaration is attached.

NOTE: For surcharge fee for filing declaration after filing date complete item VI(3) below.

NOTE: "The following combinations of information supplied in an oath or declaration filed after the filing date are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 CFR 1.63:

"(1) name of inventor(s), and application number (consisting of the series code and the serial number; e.g., 08/123,456);

"(2) name of inventor(s), serial number and filing date;

"(3) name of inventor(s) and attorney docket number which was on the specification as filed;

"(4) name of inventor(s), title which was on the specification as filed and filing date;

"(5) name of inventor(s), title which was on the specification as filed and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration; or

"(6) name of inventor(s), title which was on the specification as filed and accompanied by a cover letter accurately identifying the application for which it was intended by either the application number (consisting of the series code and the serial number; e.g., 08/123,456), or serial number and filing date. Absent any statement(s) to the contrary, it will be presumed that the application filed in the PTO is the application which the inventor(s) executed by signing the oath or declaration."

Notice of Jul. 13, 1995 (1177 O.G. 60); M.P.E.P. § 601.01(a), 6th ed., rev. 3.

NOTE: Another minimum found acceptable in the declaration is the filing date (i.e., date of express mail) and the express mail number, useful where the serial number is not yet known. But note the practice where the express mail deposit is a Saturday, Sunday or holiday within the District of Columbia. 37 C.F.R. § 1.10(c).

(complete (c) or (d), if applicable)

Attached is a

- (c) ☐ Statement by a registered attorney that the application filed in the PTO is the application that the inventor executed by signing the declaration.
- (d) ☐ Statement that the "attached" specification is a copy of the specification and any amendments thereto that were filed in the PTO to obtain the filing date.

AMENDMENT CANCELLING CLAIMS

- III. ☐ Cancel claims _____ inclusive.

TRANSMITTAL OF ENGLISH TRANSLATION OF NON-ENGLISH LANGUAGE PAPERS

- IV. ☐ Submitted herewith is an English translation of the non-English language application papers as originally filed. Also submitted herewith is a statement by the translator of the accuracy of the translation. It is requested that this translation be used as the copy for examination purposes in the PTO.

NOTE: For fee processing a non-English application, complete item VI(5) below.

NOTE: A non-English oath or declaration in the form provided by the PTO need not be translated. 37 C.F.R. § 1.69(b).

SMALL ENTITY STATUS

V.

- ☐ A statement that this filing is by a small entity

(check and complete applicable items)

- ☐ is attached.
☐ A separate refund request accompanies this paper.
☐ was filed on _____ (original).

COMPLETION FEES

VI.

WARNING: Failure to submit the surcharge fees where required will cause the application to become abandoned. 37 C.F.R. § 1.53.

NOTE: For effect on fees of failure to establish status, or change status, as a small entity, see 37 C.F.R. § 1.28(a).

1. Filing fee

- ☒ original patent application
 (37 C.F.R. § 1.16(a)— \$740 ; Small entity—\$ 370) \$ 740.00
- ☐ design application
 (37 C.F.R. § 1.16(f)— \$330 ; small entity—\$ 165) \$ _____
 \$ _____

2. Fees for claims

- ☒ each independent claim in excess of 3
 (37 C.F.R. § 1.16(b)— \$ 84 ; small entity—\$ 42) \$ 336.00
- ☒ each claim in excess of 20
 (37 C.F.R. § 1.16(c)— \$18 ; small entity—\$ 9) \$ 810.00
- ☐ multiple dependent claim(s)
 (37 C.F.R. § 1.16(d)— \$ 280 ; small entity—\$ 140) \$ _____

3. Surcharge fees

- ☒ late payment of filing fee and/or late filing of original declaration or oath
(37 C.F.R. § 1.16(e)—\$130.00; small entity—\$65.00); \$ 165.00

NOTE: Even where a facsimile declaration or oath signed by the inventor(s) was part of the originally filed papers, the surcharge fee is required.

NOTE: If both the filing fee and declaration or oath were missing from the original papers, the Office practice under § 37 C.F.R. § 1.16(e) is that only one surcharge Fee need be paid whether the later filed oath or declaration and/or the filing fee are submitted afterwards at the same time or at different times.

4. ☐ Petition and fee for filing by other than all the inventors or a person not the inventor
(37 C.F.R. §§ 1.17(i) and 1.47—\$130.00) \$ _____
5. ☐ Fee for processing an application filed with a specification in a non-English language
(37 C.F.R. §§ 1.17(k) and 1.52(d)—\$130.00) \$ _____
6. ☐ Fee for processing and retention of application
(37 C.F.R. §§ 1.21(l) and 1.53(d)—\$130.00) \$ _____
7. ☒ Assignment (See "ASSIGNMENT COVER SHEET".)

NOTE: 37 C.F.R. § 1.21(l) establishes a fee for processing and retaining any application which is abandoned for failing to complete the application pursuant to 37 C.F.R. § 1.53(f) and this, as well as, the changes to 37 C.F.R. §§ 1.53 and 1.78 indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee or the processing and retention fee of § 1.21(l) within 1 year of notification under § 1.53(f) must be paid.

Total completion fees \$ 1932.00

EXTENSION OF TIME**VII.**

(complete (a) or (b), as applicable)

The proceedings herein are for a patent application, and the provisions of 37 C.F.R. § 1.136(a) apply.

- (a) ☐ Applicant petitions for an extension of time, the fees for which are set out in 37 C.F.R. § 1.17(a)(1)-(4), for the total number of months checked below:

Extension (months)	Fee for other than small entity	Fee for small entity
<input type="checkbox"/> one month	\$ 110.00	\$ 55.00
<input type="checkbox"/> two months	\$ 400.00	\$ 200.00
<input type="checkbox"/> three months	\$ 920.00	\$ 460.00
<input type="checkbox"/> four months	\$1440.00	\$ 720.00

Fee \$ _____

If an additional extension of time is required, please consider this a petition therefor.

(check and complete the next item, if applicable)

- ☐ An extension for _____ months has already been secured, and the fee paid therefor of \$_____ is deducted from the total fee due for the total months of extension now requested.

Extension fee due with this request \$_____

or

- (b) ☒ Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

TOTAL FEE DUE

VIII.

The total fee due is

Completion fee(s) \$ 1932.00

Extension fee (if any) \$ _____

Total Fee Due \$ 1932.00

PAYMENT OF FEES

IX.

- ☒ Enclosed is a check in the amount of \$ 1972.00 which includes \$40 for assignment recordation.
- ☐ Charge Account No. _____ in the amount of \$_____.
- A duplicate of this request is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 C.F.R. § 1.22(b).

Please charge Account No. _____ for any fees that may be due by this paper

AUTHORIZATION TO CHARGE ADDITIONAL FEES

X.

WARNING: Accurately count claims, especially multiple dependant claims, to avoid unexpected high charges if extra claims are authorized.

NOTE: "Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account." 37 C.F.R. § 1.26(a).

- ☒ The Commissioner is hereby authorized to charge the following additional fees that may be required by this paper and during the pendency of this application to Account No. 23-0442

☒ 37 C.F.R. § 1.16(a), (f) or (g) (filing fees)

☐ 37 C.F.R. § 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.

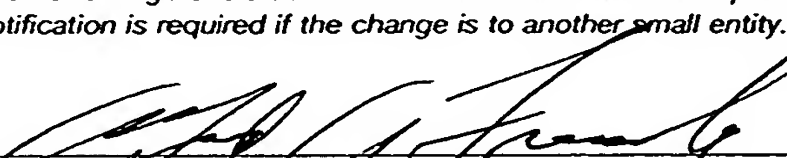
- ☒ 37 C.F.R. § 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)
- ☒ 37 C.F.R. § 1.17(a)(1)-(5) (extension fees pursuant to § 1.136(a))
- ☐ 37 C.F.R. § 1.17 (application processing fees)

NOTE: "A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).

- ☐ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying . . . issue fee . . ." From the wording of 37 C.F.R. § 1.28(b): (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.



SIGNATURE OF PRACTITIONER

Alfred A. Fressola

(type or print name of practitioner)

WARE, FRESSOLA, VAN DER SLUYS & ADOLPHSON LLI
755 Main Street, Building Five

P.O. Address
Box 224
Monroe, CT 06468

Reg. No. 27,550

Tel. No.: (203) 261-1234

Customer No. 04955



COMBINED DECLARATION AND POWER OF ATTORNEY

(Docket Number)

944-005.2

As a below named inventor, I hereby declare that:

- my residence, post office address and citizenship are as stated below next to my name;
- I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Method and System for User Generated Keys and Certificates**
- the specification of which is attached hereto unless the following box is checked: ☒. If the box is checked,

the application was filed on **February 28, 2002**

as U.S. Application Number **10/090,422**

or PCT International Application Number

and was amended on (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application			Priority Not Claimed
(Application Number)	(Country)	(Day/Month/Year Filed)	<input type="checkbox"/>
(Application Number)	(Country)	(Day/Month/Year Filed)	<input type="checkbox"/>
(Application Number)	(Country)	(Day/Month/Year Filed)	<input type="checkbox"/>

To the extent permitted by rule or law, I hereby incorporate by reference the Prior Foreign Application(s) listed above.

I hereby claim the benefits under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

(Provisional Application Number)	(Day/Month/Year Filed)
(Provisional Application Number)	(Day/Month/Year Filed)

I hereby claim the benefit under 35 U.S.C. §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information which is material to patentability, as defined in 37 CFR §1.56, which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Application Number)	(Day/Month/Year Filed)	(Status--patented, pending, abandoned)
(Application Number)	(Day/Month/Year Filed)	(Status--patented, pending, abandoned)

I hereby appoint the attorney(s) and/or agent(s) assigned to the customer number listed below, as may from time to time be amended, belonging to the firm of Ware, Fressola, Van Der Sluys & Adolphson LLP, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer Number

4955



004955

PATENT AND TRADEMARK OFFICE

Address all telephone calls to: Ware, Fressola, Van Der Sluys & Adolphson LLP at (203) 261-1234. Address all correspondence to: Alfred A. Fressola

Customer Number

4955



004955

PATENT AND TRADEMARK OFFICE

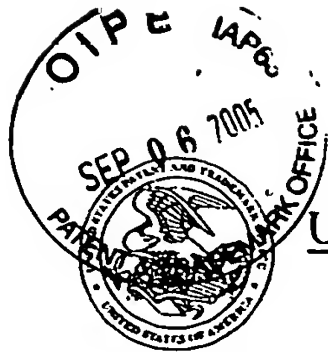
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Lauri PAATERO Full name of sole or first inventor (given name, middle initial, FAMILY NAME(S) IN UPPER CASE)	
<u>Lauri Paatero</u> Inventor's Signature	<u>18-Apr-2002</u> Date
00970 Helsinki, Finland Residence	Finnish Citizenship
Post Office Address: Rikalantie 4, 00970 Helsinki, Finland	

Full name of second inventor (given name, middle initial, FAMILY NAME(S) IN UPPER CASE)	
_____ Inventor's Signature	_____ Date
_____ Residence	_____ Citizenship
Post Office Address:	

Full name of third inventor (given name, middle initial, FAMILY NAME(S) IN UPPER CASE)	
_____ Inventor's Signature	_____ Date
_____ Residence	_____ Citizenship
Post Office Address:	

☐ Additional inventors are being named on separately numbered sheets attached hereto.



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/090,422	02/28/2002	Lauri Paatero	944-005.002

004955
WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

CONFIRMATION NO. 6221

FORMALITIES LETTER



OC000000007788412

Date Mailed: 04/04/2002

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

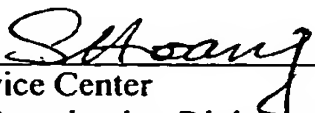
FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
Applicant must submit \$ 370 to complete the basic filing fee for a small entity.
- Total additional claim fee(s) for this application is \$531.
 - \$405 for 45 total claims over 20.
 - \$126 for 3 independent claims over 3 .
- The oath or declaration is missing.
A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(l) of \$65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.
- The balance due by applicant is \$ 966.

*A copy of this notice **MUST** be returned with the reply.*


Customer Service Center
Initial Patent Examination Division (703) 308-1202

PART 2 - COPY TO BE RETURNED WITH RESPONSE